CLAIMS

Please amend the claims as follows:

Claims 1-53 are cancelled.

54.   (Currently amended) A method, comprising:

determining at a local server whether a user is authorized to access a remote server;

when the user is authorized, identify at the local server a privilege level associated with the user, the identified privilege level defining how the user is permitted to control an <u>Operating System (OS) installed</u> ~~operating system running~~ on the remote server;

<u>logging the local server onto the OS, said login using a first account that gives the local server unrestricted administrative access to the OS installed on the remote server, said unrestricted login being non-corresponding with the identified privilege level;</u>

receiving at the local server one or <u>more</u> commands from the user, the commands for controlling the <u>OS</u> ~~operating system~~;

filtering the commands received at the local server according to a verification of whether the received commands correspond to the identified privilege level for the user; and

sending messages that represent the filtered commands from the local server, over a packet switched network, and to the remote server when the commands correspond to the identified privilege level[[.]]<u>;</u>

<u>wherein at least one of the received commands is blocked through the filtering by the local server, the blocked command being one that is permissible with unrestricted administrative access such that said filtering and sending by the local server simulates user logon using a second different account having restricted administrative privileges to the OS installed on the remote server while the local server is actually logged onto, and accessing, the remote server using the first account having unrestricted administrative privileges.</u>

55.   (Currently amended) The method of claim 54 <u>wherein</u> ~~further comprising logging into the remote server prior to sending the messages,~~ said <u>logon</u> ~~login~~ <u>is</u> conducted using an operating system level account that is selected independently of the user.

56.   (Previously Presented) The method of claim 54 wherein the messages are sent using a transfer protocol that operates independently of HyperText Transfer Protocol (HTTP) capability on the remote server and that operates independently of TELecommunications NETwork (TELNET) capability on the remote server.

57.   (Previously Presented) The method of claim 54 wherein the commands are generated in response to the user making selections on one or more web pages displayed by a client system.

58.   (Previously Presented) The method of claim 54 wherein the messages cause the remote server to download files to a client system separate from the remote server.

59.   (Previously Presented) The method of claim 58 wherein the client system is a same client system that originates the commands.

60.   (Previously Presented) The method of claim 54 further comprising the local server creating a session log entry that identifies the commands represented by the messages, the session log entry containing information allowing a system administrator to undo transactions performed on the remote server.

61.   (Previously Presented) The method of claim 60 wherein the transactions alter a file system stored on the server and the session log entry allows the system administrator to rebuild the file system.

62.   (Currently amended) A system, comprising:

a content server having configured thereon an Operating System (OS) , the OS capable of provisioning different OS logon ~~level~~ accounts that define different levels of administrative privileges for different users;

the content server having established thereon an OS logon account configured to allow a first range of administrative privileges to a logged on user ~~a single OS level account for allowing access to a plurality of remote users, the single OS level account associated a same level of administrative privileges for the remote users~~;

one or more central servers to function as a trusted proxy for the content server by remotely administering privilege management for the content sever, the central servers to log onto the OS using the established OS logon account that provides the first range of administrative privileges;

the central servers to receive an access request from one of the remote users, to determine whether the remote user is authorized to access the content server, and when the remote user is authorized to access the content server, to select a level of administrative privileges according to the remote user; and

the central servers to receive, from an endpoint for the remote user, commands for controlling the content server, to filter the received commands according to the selected level of administrative privileges such that the user can be restricted to a second range of administrative privileges, the second range being a subset of the first range of administrative privileges, and to forward the filtered commands to the content server while the central server is logged onto the content server using the OS logon account having the first range of administrative privileges.

63.   (Currently amended) The system of claim 62 wherein the ~~single~~ OS logon ~~level~~ account is a generic account that does not restrict administrative privileges, and the central servers impose administrative privilege level ~~differing~~ restrictions on the remote users through command filtering.

64.   (Currently amended) The system of claim 62 wherein the central servers are logged onto the content server under the ~~single~~ OS logon ~~level~~ account when forwarding the filtered commands for the different users.

65. (Previously Presented) The system of claim 62 wherein the commands are generated by the remote user interacting with a web browser and are formatted as HyperText Transfer Protocol (HTTP) requests, and the server forwards the commands using an File Transfer Protocol (FTP) format.

66. (Previously Presented) The system of claim 62, further comprising:

the central server to send a notification to the remote user when one of the commands is filtered, the notification indicating that the remote user does not have a requisite level of administrative privileges to control the content server using the filtered command.

67. (Previously Presented) The system of claim 62, wherein the content server performs transactions according to the forwarded commands and the system further comprises:

the central server to create one or more session log entries that identify the forwarded commands, the session log entries containing information allowing a system administrator to undo the transactions.

68. (Previously Presented) The system of claim 67 wherein the transactions alter a file system stored on the content server and the session log entry allows the system administrator to rebuild the file system.

69. (Previously Presented) The system of claim 62 wherein the received commands are for creating files and directories, editing files and directories, or removing files and directories.

70. (Previously Presented) The system of claim 62 wherein a file structure on the content server is manipulated according to the forwarded commands.

71. (Currently amended) The system of claim 62 wherein the OS ~~operating system~~ is an embedded OS ~~operating system~~.

72.   (Previously Presented) An apparatus, comprising:

one or more processors; and

a memory coupled to the processors comprising instructions executable by the processors, the processors operable when executing the instructions to:

establish a connection through a packet switched network and to a server;

log onto an Operating System (OS) of the server using a single Operating System (OS) level account that is established on the server;

receive commands from a plurality of different users, the commands for controlling the server;

for each command, identify a user associated with the command, compare the associated user to a database that identifies differing levels of administrative privileges for the different users, and filter the command according to the identified level of administrative privileges for the associated user; and

while remaining logged onto the server using the single OS level account, forward the filtered commands from the different users over the connection to the server.

73.   (Previously Presented) The apparatus of claim 72 wherein the apparatus offloads, from the server, managing which of the different users are able to control which functionality of the OS.

74.   (Previously Presented) The apparatus of claim 73 wherein the apparatus allows the different users to control the OS independently of whether a password for logging into the OS is provided to the users.

75.   (Previously Presented) The apparatus of claim 74 wherein the apparatus allows the server to maintain only a single OS level account and password regardless of the number of remote users.

76. (New) An apparatus operable to:

log onto an Operating System (OS) of a remote server using an Operating System (OS) logon account existing on the remote server, the OS logon account providing a first range of administrative privileges for configuring the OS;

receive commands from a plurality of different users, the commands for controlling the remote server;

for each command, identify a user associated with the command, compare the associated user to a database that identifies differing ranges of administrative privileges for the different users, and filter the command according to the identified level of administrative privileges for the associated user; and

while remaining logged onto the server using the OS logon account, forward the filtered commands from the different users over the connection to the server;

wherein at least one of the identified level of administrative privileges provides a second range of administrative privileges, wherein the second range is a subset of the first range.

77. (New) The apparatus of claim 76 wherein said filtering causes commands for installing a patch on the remote server to be forwarded if originating from a first user and filtered if originating from a second different user.

78. (New) The apparatus of claim 76 wherein said filtering causes commands for reconfiguring installed software on the remote server to be forwarded if originating from a first user and filtered if originating from a second different user.

79. (New) The apparatus of claim 78 wherein forwarded commands from two users are processed by the OS as if the forwarded commands were generated by a single logged on entity.